REMARKS

Claims 1-14 were pending when the Application was examined. Claims 1, 3, 6-8, 11, 12 and 14 are amended for reasons unrelated to patentability. New claim 15 is added. Claims 1-15 are now pending, of which, claims 1, 3, 6, 8, 11, 12 and 14 are independent.

The specification and the claims are amended to change the term "multiplexer" to "multiplier." This change pertains to correcting a mistranslation from the priority parent application and does not introduce new matter.

Claim Rejections 35 U.S.C. 102(e)

Claims 1-14 are rejected under 35 U.S.C. 102(e) as allegedly anticipated by Van Buer (U.S. Patent Application Publication No. 2003/0198345).

Applicant amends the claims as shown above, traverses the rejections as follows, and submits that the claims would be patentable even without the amendments.

Claim 1

Claim 1 recites "An AES encryption processor comprising: a selector unit selecting an element of a state in response to row and column indices; a substitution unit for obtaining a substitution value with said selected element used as an index; a coefficient table providing first to fourth coefficients in response to said row index; first to fourth multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients, respectively, the first to fourth products corresponding to a same one column of the state; and an accumulator which accumulates the first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designated column of a resultant state." (Emphasis added.)

Claim 1 is amended merely to improve form and not to narrow the scope of the claim.

Support for the amendments may be found throughout the specification and drawings and, for example, in figure 9 of the drawings and in paragraphs 104 and 106 of the published Application. (U.S. Patent Application Publication No. 2004/0184602.)

Applicant submits that Van Buer does not teach or suggest "a coefficient table providing first to fourth coefficients in response to said row index" or "first to fourth multipliers ... computing first to fourth products, which are obtained by multiplication of said substitution value with the first to fourth coefficients" or "an accumulator ... to develop first to fourth elements of ... a resultant state" of claim 1.

Van Buer appears to be based on parallel processing. Figure 3 of Van Buer shows a number of substitution boxes or S-boxes, S1 through S16, being used in parallel to process 16 octets of the input data that may correspond to the 16 elements of the 4 by 4 state matrix. The parallel nature of processing in Van Buer is emphasized in paragraph 63 of this reference "processing the entire block 120 in parallel, as illustrated in FIG. 3." (Van Buer, paragraph 63.)

With using one S-box for each element of state, as done in Van Buer, there is no need to use "an accumulator ... to develop first to fourth elements of a designated column of a resultant state" as claimed in claim 1 or the parts that provide the input to the "accumulator," namely the "coefficient table" or the "first to fourth multipliers" of claim 1. (See also paragraph 106 of the published Application discussing one of the features of the Application: "The architecture in this embodiment effectively reduces necessary hardware while achieving the parallel processing. The coefficient table 106, the multipliers 107_0 to 107_4, and the adder 109 eliminate the need for preparing a plurality of S-boxes (or expanded S-boxes) for implementing parallel processing in connection with a single column of the output state.")

The Office action is citing to paragraphs 55 and 63 of Van Buer for teaching the "coefficient table" of claim 1. (Office action, p. 3.)

Paragraph 55 of Van Buer is repeated below:

> Rijndael and AES can in principle be implemented in completely unclocked logic. The relationship between the inputs and the output can be entirely composed of exclusive-or, reordering, multiplexers and substitution tables. However this could result in data flow consecutively through a long cascade on the order of 100 gates where every output is a function of every input. Within a pipeline, the throughput per clock cycle can be increased by introducing synchronously clocked latches at key points along the pipeline. By doing this, each clocked stage can be constructed to perform a part of the encryption or decryption for a different key and data block.

(Emphasis added.)

Latches of Van Buer appear to store the results of each part of the pipeline and release them synchronously. Key latches and data latches are shown in figures 28 through 38 of Van Buer. These latches seem to be synchronizing keys and data along two parallel paths in pipelines or causing rounds to skip key expansions. (See, Van Buer, paragraph 98.) There is no table in these figures and no relationship to the indices of the state matrix is shown. As such, Applicant fails to see to how these latches teach the "a coefficient table providing first to fourth coefficients in response to said row index" of claim 1. (See also, paragraph 118 of the published Application stating, regarding the second embodiment, that "auxiliary registers … are provided for pipeline processing … should not be understood as … essential for the AES encryption …." Emphasis added.)

The cited paragraph 63 of Van Buer is repeated below:

> The output of the exclusive-or circuit 114 of FIG. 2 can be a data block of the same width as was in block 110, which can form an input 120 to a substitution circuit 122, as shown in more detail in FIG. 3. The input data block can be treated as a series of 8-bit octets A, B, C . . . to P in the case of 128 bits, i.e., 16

> octets, A, B, C . . . XH, in the case of 192 bits, i.e., 24 octets and A, B, C . . . XP in the case of 256 bits, i.e., 32 octets. Each octet can be used as an index into a substitution table (or inverse table during decryption), and the output into data block 124 can be the octet value in the table within the respective S-Box, e.g., S1 . . . S16, i.e., the A, B, C . . . P in the substitution stage data block 124. Such a look-up table is referred to herein as an S-Box S1, S2, S3 . . . S16 or S24 or S32. Because the octets are independent in this step, maximum speed can be achieved by providing, e.g., 32 copies of the respective S-Boxes, S1 . . . S32, for 256-bit Rijndael data blocks, or, e.g., 16 copies of the table S1 . . . S16, for 128-bit AES, which can be implemented, e.g., as a read-only memory, and processing the entire block 120 in parallel, as illustrated in FIG. 3.

(Emphasis added.)

This paragraph of Van Buer appears to pertain to the substitution boxes or S-boxes. Claim 1 already includes "a substitution unit for obtaining a substitution value with said selected element used as an index" that is apart from the "coefficient table providing first to fourth coefficients in response to said row index" in the context of claim 1.

Paragraphs 54, 55, 58, 63 and 64 of Van Buer are cited for teaching the "first to fourth multiplexers (multipliers) … computing first to fourth products … obtained by multiplication of said substitution value with the first to fourth coefficients" of claim 1. (Office action, p. 4.) However, these passages of Van Buer neither teach "multiplexers (multipliers) … computing first to fourth products," nor help clarify what is cited against the "coefficient table" of claim 1. Paragraph 54 of Van Buer is about the relationship between the length of an encryption pipeline, in rounds, and skipping rounds in order to obtain the desirable number of rounds of encryption given the particular pipeline length. Paragraph 58 is again about adding independent pipelines to increase the throughput of a pipelined encryption. Finally, paragraph 64, like paragraph 63 cited above, is about the substitution box or S-box which is separate from the "coefficient table" and the multiplexers or "multipliers … computing first to fourth products" of claim 1.

Paragraphs 67 to 69 of Van Buer are cited against "an accumulator which accumulates the first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designated column of a resultant stat" of claim 1. (Office action, p. 3.)

However, paragraphs 67 to 69 of Van Buer that describe figure 4 of this reference, appear to pertain to operations performed on one element of the state matrix. Figure 3 of Van Buer already showed that in Van Buer, there is one element per one S-box. So, figure 4 includes one "input octet" that goes through the single S-box 152. If there is any accumulation in figure 4, it is at the multiplexers 154 and 158 that are just adding the octet to its inverse affine 164 or to its affine transform 160. Finally, the result of the entire pipeline is still one element: "The second multiplexer 158 determines the proper output, the result of the S-box 152 for decryption or the output of the affine function performed in box 160 for encryption." (Van Buer, figure 4, paragraph 58.) Therefore, there is no teaching or suggestion of an "accumulator" that has to do with "first to fourth products corresponding to all four columns of the state to develop first to fourth elements of a designated column of a resultant state" of claim 1 in the cited passages of Van Buer. (Emphasis added.)

As such, none of the cited portions of Van Buer appear to teach or suggest the "coefficient table" or "first to fourth multipliers ... computing first to fourth products" or the "accumulator" of claim 1.

Accordingly, claim 1 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 3

Claim 3 recites in part "a coefficient table providing first to fourth coefficients in response to said row index; first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively."

As explained above, at least the "coefficient table" and the "Galois field multipliers" of claim 3 are not taught or suggested by Van Buer.

Accordingly, claim 3 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 6

Claim 6 recites in part "a coefficient table providing first to fourth coefficients in response to said row index; first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively."

As explained above, at least the "coefficient table" and the "Galois field multipliers" of claim 6 are not taught or suggested by Van Buer.

Accordingly, claim 6 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 8

Claim 8 recites in part "a coefficient table providing first to fourth coefficients in response to said immediate operand; first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively."

As explained above, at least the "coefficient table" and the "Galois field multipliers" of claim 8 are not taught or suggested by Van Buer.

Accordingly, claim 8 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 11

Claim 11 recites in part "a coefficient table providing first to fourth coefficients in response to said row index; first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients, respectively."

As explained above, at least the "coefficient table" and the "Galois field multipliers" of claim 11 are not taught or suggested by Van Buer.

Accordingly, claim 11 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 12

Claim 12 recites in part "a coefficient table providing first to fourth coefficients in response to said row index; first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients."

As explained above, at least the "coefficient table" and the "Galois field multipliers" of claim 12 are not taught or suggested by Van Buer.

Accordingly, claim 12 is not anticipated by Van Buer and is believed to be patentable over this reference.

Claim 14

Claim 14 recites in part "first to fourth Galois field multipliers respectively computing first to fourth products, which are obtained by multiplication of said substitution value with first to fourth coefficients."

As explained above, at least the "first to fourth coefficients" and the "Galois field multipliers" of claim 14 are not taught or suggested by Van Buer.

Accordingly, claim 14 is not anticipated by Van Buer and is believed to be patentable over this reference.

Dependent Claims

Claims 2 and 15 depend from claim 1. Claims 4-5 depend from claim 3. Claim 7 depends from claim 6. Claims 9-10 depend from claim 8. Claim 13 depends from claim 12.

Applicant submits that the dependent claims are believed to be patentable at least for depending from patentable independent claims.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.

Respectfully submitted,

/fariba sirjani/

Fariba Sirjani
Registration No. 47,947

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: January 16, 2009